

**Robert A Kalka Metropolitan Skyport**

**Penetration Test Report**

January 12-13, 2024

Finals-##

**Confidentiality Notice**

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. The publication of this report may cause reputational damage to Robert A Kalka Metropolitan Skyport (RAKMS) or facilitate attacks against RAKMS. <TEAM NAME> shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.

**Disclaimer**

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on RAKMS’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

**Document Control Details**

Company: Robert A Kalka Metropolitan Skyport (RAKMS)

Version: 1.0

Last Edited: January 13, 2024

Prepared By: TEAM-##

Classification: Confidential

**Document Recipients**

NAME, TITLE - MONTH DAY, YEAR

Table of Contents

[1.0 Assessment Overview 5](#_Toc155784677)

[1.1 Executive Summary 5](#_Toc155784678)

[1.2 Reassessment Summary 7](#_Toc155784679)

[1.3 Technical Findings Summary 9](#_Toc155784680)

[2.0 Engagement Details 10](#_Toc155784681)

[2.1 Scope 10](#_Toc155784682)

[2.2 Network Topology 10](#_Toc155784683)

[2.3 Engagement Narrative 11](#_Toc155784684)

[2.3.1 Pre-engagement 11](#_Toc155784685)

[2.3.2 Friday, January 12th, 2024 11](#_Toc155784686)

[2.3.3 Saturday, January 13th, 2024 11](#_Toc155784687)

[3.0 Compliance 12](#_Toc155784688)

[4.0 Strategic Recommendations 13](#_Toc155784689)

[4.1 Key Security Strengths 13](#_Toc155784690)

[4.1.1 Strength 1 13](#_Toc155784691)

[4.1.2 Strength 2 13](#_Toc155784692)

[4.1.3 Strength 3 13](#_Toc155784693)

[4.2 Key Findings & Recommendations 13](#_Toc155784694)

[4.2.1 Finding 1 13](#_Toc155784695)

[4.2.2 Finding 2 13](#_Toc155784696)

[4.2.3 3 13](#_Toc155784697)

[5.0 Technical Findings 14](#_Toc155784698)

[5.1 Critical Vulnerabilities 14](#_Toc155784699)

[C.1 Vulnerability Name 14](#_Toc155784700)

[5.2 High Vulnerabilities 16](#_Toc155784701)

[H.1 High Vulnerability 16](#_Toc155784702)

[5.3 Medium Vulnerabilities 17](#_Toc155784703)

[M.1 Medium Vulnerability 17](#_Toc155784704)

[5.4 Low Vulnerabilities 18](#_Toc155784705)

[L.1 Low Vulnerability 18](#_Toc155784706)

[5.5 Informational Vulnerabilities 19](#_Toc155784707)

[I.1 Informational Vulnerability 19](#_Toc155784708)

[6.0 Appendix A: Methodology 20](#_Toc155784709)

[7.0 Appendix B: Risk Assessment Metrics 21](#_Toc155784710)

[7.1 Risk Matrix 21](#_Toc155784711)

[7.2 Classification Definitions & Scales 21](#_Toc155784712)

[7.2.1 Impact 21](#_Toc155784713)

[7.2.2 Likelihood 22](#_Toc155784714)

[7.2.3 Remediation 22](#_Toc155784715)

[8.0 Appendix C: Open-Source Intelligence 23](#_Toc155784716)

[9.0 Appendix D: Social Engineering Engagement 24](#_Toc155784717)

[9.1 Voice-Phishing Assessment 24](#_Toc155784718)

[9.2 Phishing Assessment 24](#_Toc155784719)

[10.0 Appendix E: RF Assessment 25](#_Toc155784720)

[11.0 Appendix F: Network Details 26](#_Toc155784721)

[11.1 Network 1 26](#_Toc155784722)

[11.2 Network 2 26](#_Toc155784723)

[12.0 Appendix G: Tools 27](#_Toc155784724)

# Assessment Overview

## Executive Summary

**Overview**

TEAM performed a penetration test on RAKMS’s BLANK network(s) on January 12-13, 2024. The penetration test simulated an attack of an internal threat actor attempting to gain access to RAKMS network systems. The purpose of the penetration test was to discover network strengths, vulnerabilities, suggest remediations to improve RAKMS’s cybersecurity posture, and to assess how RAKMS’s security posture has changed since the previous assessment on October 14, 2023.

TEAM identified strengths including STRENGTH 1, STRENGTH 2, and STRENGTH 3. These strengths improved security across various points of the tested network.

**Reassessment Findings**

Finals-##’s re-evaluated all previously identified vulnerabilities to assess RAKMS’s remediation efforts. Of the # previously identified vulnerabilities, # have been remediated, # have been partially remediated, and # have not been remediated.

**Vulnerability Findings**

TEAM identified a total of # vulnerabilities within the scope of the engagement, which are broken down by severity in the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Informational** |
| **#** | **#** | **#** | **#** | **#** |

**Critical Vulnerabilities**

Paragraph about critical vulnerabilities…

**Compliance**

Paragraph about compliance….

**Key Opportunities for Improvement**

Key opportunities for improvement….

## Reassessment Summary

One of Finals-##’s primary goals of this second penetration assessment was to assess how RAKMS’s security posture has changed since the previous assessment conducted on October 14, 2023. In addition to testing for unidentified vulnerabilities, the consultants re-evaluated all of the vulnerabilities found during the prior penetration test to provide detailed information about RAKMS’s remediation efforts. Out of the 16 previous findings, 1 finding has been successfully remediated, 3 findings were partially remediated, 7 findings need to be remediated, and 5 findings were not applicable.

The table below indicates the remediation status for each previously identified vulnerability:

|  |  |  |
| --- | --- | --- |
| **Finding Name** | **Severity Level** | **Remediation Status** |
|  | Critical |  |
|  | Critical |  |
|  | High |  |
|  | High |  |
|  | High |  |
|  | High |  |
|  | High |  |
|  | High |  |
|  | Medium |  |
|  | Medium |  |
|  | Medium |  |
|  | Medium |  |
|  | Medium |  |
|  | Medium |  |
|  | Medium |  |
|  | Low |  |
|  | Low |  |
|  | Low |  |
|  | Low |  |
|  | Informational |  |
|  | Informational |  |
|  | Informational |  |

## Technical Findings Summary

The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in [Appendix B](#_Appendix_B:_Risk).

During the penetration test, TEAM-## uncovered a total of # findings that pose a material risk to RAKMS’s information systems. TEAM-## also identified # informational findings that, if addressed, could further strength RAKMS’s overall security posture. The informational findings do not represent security vulnerabilities on their own, they are observations for areas of improvement by the organization. The below table provides a summary of the findings by severity level.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Informational** |
| **#** | **#** | **#** | **#** | **#** |

The below table provides a high-level overview of each finding identified during testing. These findings are covered in depth in the Assessment Findings Details section of this report.

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | **Severity Level** | **Finding Name** | **Page #** |
| C1 | Critical |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Engagement Details

## Scope

The scope of this penetration testing assessment included…

Internal testing was done during the testing window of…

|  |  |
| --- | --- |
| **IP Address/Host/URL** | **Description** |
|  |  |

Provided Credentials

|  |  |
| --- | --- |
| **Username** | **Description** |
|  |  |

## Network Topology

## Engagement Narrative

### Pre-engagement

### Friday, January 12th, 2024

### Saturday, January 13th, 2024

# Compliance

### TSA Security Directives

### PCI DSS

# Strategic Recommendations

## Key Security Strengths

### Strength 1

### Strength 2

### Strength 3



## Key Findings & Recommendations

### Finding 1

### Finding 2

### 3



# Technical Findings

This section provides a detailed description for each finding uncovered during the penetration test of RAKMS’s in-scope technology systems. The findings are organized based on severity level (Critical, High, Medium, Low, Informational).

The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in [Appendix B](#_Appendix_B:_Risk).

## Critical Vulnerabilities

1. Vulnerability Name

|  |  |
| --- | --- |
| **Critical Risk** | |
| **Likelihood** | Likely |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

## High Vulnerabilities

1. High Vulnerability

|  |  |
| --- | --- |
| **High Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

## Medium Vulnerabilities

1. Medium Vulnerability

|  |  |
| --- | --- |
| **Medium Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Severe |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

## Low Vulnerabilities

1. Low Vulnerability

|  |  |
| --- | --- |
| **Low Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Moderate |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

**END OF FINDING**

## Informational Vulnerabilities

1. Informational Vulnerability

|  |  |
| --- | --- |
| **Informational Risk** | |
| **Likelihood** | Unlikely |
| **Impact** | Minor |
| **Remediation** | Hard |

Affected Scope



Description

Description of the vulnerability

Steps to Reproduce

How you determined there was a vulnerability, what you saw, proof of concept, detailed steps

Technical Impact

Technical consequences that would result due to exploitation.

Business Impact

Business consequences that would result due to exploitation.

Remediation Recommendation

Sdffsdafsdfsdfsdaf

References

Ref 1

END OF FINDING

# Appendix A: Methodology

TEAM’s testing methodology had three main phases - reconnaissance, target assessment, and execution of assessment. Reconnaissance involved conducting Open-Source Intelligence (OSINT) research to gather publicly available information about RAKMS and network enumeration scans to gather information on available hosts and the network topology. The consultants used tools such as Nmap to identify systems and service versions of hosts and applications on the networks. Manual vulnerability scans were also conducted during the target assessment phase. For execution of assessment, the consultants used tools such as Burp Suite, Metasploit, and Hydra to find and exploit vulnerabilities. The diagram below shows a visual representation of the testing methodology the consultants followed throughout the penetration test.

A diagram of a target assessment

Description automatically generated

## Open Web Application Security Project (OWASP)

TEAM utilized the [OWASP Top 10](https://owasp.org/Top10/) to evaluate RAKMS web applications, aiming to pinpoint typical vulnerabilities and misconfigurations. The 2021 Version of OWASP Top 10 Consists of the following:

|  |  |
| --- | --- |
| OWASP Top Ten 2021 | |
| [Broken Access Control](https://owasp.org/Top10/A01_2021-Broken_Access_Control/) |  |
| [Cryptographic Failures](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/) |  |
| [Injection](https://owasp.org/Top10/A03_2021-Injection/) |  |
| [Insecure Design](https://owasp.org/Top10/A04_2021-Insecure_Design/) |  |
| [Security Misconfiguration](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/) |  |
| [Vulnerable and Outdated Components](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/) |  |
| [Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) |  |
| [Security Logging and Monitoring Failures](https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/) |  |
| [Server-Side Request Forgery](https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/) |  |

# Appendix B: Risk Assessment Metrics

## Risk Matrix

TEAM-## utilized the following 3x3 risk matrix for determining the severity level of each finding uncovered during the assessment. After determining the impact and likelihood classifications for the finding, they are used to select the appropriate severity level based on the risk matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Impact** | | |
|  |  | Severe | Moderate | Minor |
| **Likelihood** | Likely | Critical | High | Medium |
| Possible | High | Medium | Low |
| Unlikely | Medium | Low | Informational |

## Classification Definitions & Scales

TEAM-## utilized the following definitions and scales for classifying impact, likelihood, and remediation for each finding.

### Impact

**Definition:** With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Severe | Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage. |
| Moderate | Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions. |
| Minor | Successful exploitation of the vulnerability may affect a few users without causing much disruption to routine functions. |

### Likelihood

**Definition:** A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Likely | Exploitation methods are well-known and can be performed with minimal difficulty using publicly available tools. |
| Possible | Exploitation methods are well-known and may be performed using public tools with configuration changes. Understanding of the underlying system is required for successful exploitation. |
| Unlikely | Exploitation requires deep understanding of the underlying system or advanced technical skills. Precise conditions may be required for successful exploitation. |

### Remediation

**Definition:** The act of mitigating a vulnerability or a threat.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Hard | Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions. |
| Medium | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| Easy | Remediation may be accomplished within a short amount of time and with little difficulty. |

# Appendix C: Open-Source Intelligence

# Appendix D: Social Engineering Engagement

## Voice-Phishing Assessment

## Phishing Assessment

# Appendix E: RF Assessment

# Appendix F: Network Details

## Network 1

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **FQDN** | **Port(s)** | **Services** |
|  |  |  |  |
|  |  |  |  |

## Network 2

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **FQDN** | **Port(s)** | **Services** |
|  |  |  |  |
|  |  |  |  |

# Appendix G: Tools

|  |  |
| --- | --- |
| **Name** | **Description** |
| Burp Suite | A Java based Web Penetration Testing framework that is a integrated platform for performing security testing of web applications. |
| CrackMapExec | CME is a wrapper tool for the window’s offensive security tool suite Impacket and is used to enumerate and escalate privileges in a domain. |
| Hashcat | A password cracking tool used for password recovery. |
| Hydra | Hydra is used for credential stuffing and password spraying against SSH. |
| Impacket | A python-based Windows protocol suite used for offensive security testing in Windows domains. |
| Metasploit | An offensive security tool database used for exploiting known or common vulnerabilities. |
| Maltego | Maltego is an OSINT Aggregation tool suite that allows for the graphical representation the links between disparate piece of information |
| Netdiscover | Netdiscover is a tool used for network device enumeration using passive and active ARP capture techniques. |
| Nmap | Nmap enumerate devices and services on a network using a variety of techniques such as TCP SYN-scanning, ICMP echo scanning, and reverse name resolution. |
| Pacu | Pacu is an Amazon Web Services exploitation framework used to enumerate and exploit AWS resources. |
| PetitPotam | PetitPotam is the name of both a vulnerability and tool used to coerce a Windows server to authenticate to an attacker-controlled computer. |
| PKINITtools | PKINITtools are tools for Kerberos Public Key Cryptography for Initial Authentication (PKINIT) and relaying to AD CS. |
| Responder | A Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS) and Multicast Domain Name System (MDNS) poisoner. |
| Wappalyzer | A technology profiler that shows what websites are built with. |
| WhatWeb | WhatWeb identifies software used in web pages through signature matching and common web directories. |
| Winpeas | Winpeas is a post exploitation tool that helps testers automate discovering local privilege escalation vectors and sensitive data. |

Red #FF7D7D

Orange #F4B083

Yellow #FFFF99

Green #A8D08D

Blue #D9E2F3